1

2


Wizard of Oz
Sing Along & Character Look Alike

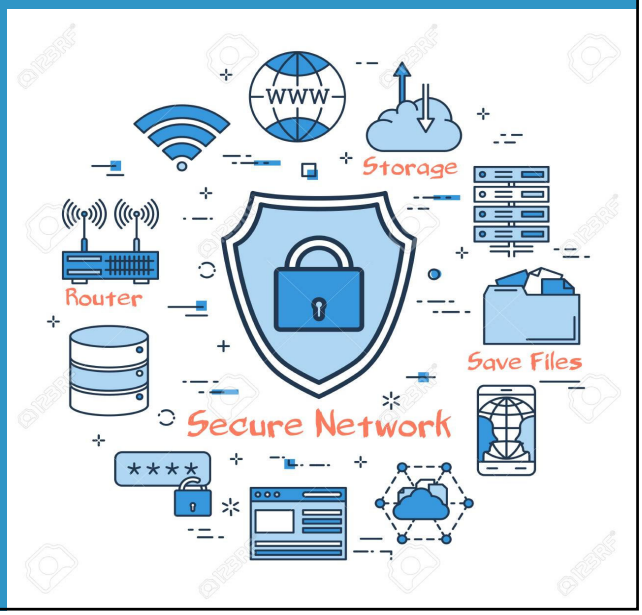
3


Breaches and Ransoms and Phish, Oh My!
HEARTLAND
BUSINESS SYSTEMS

4

THE DESTINATION

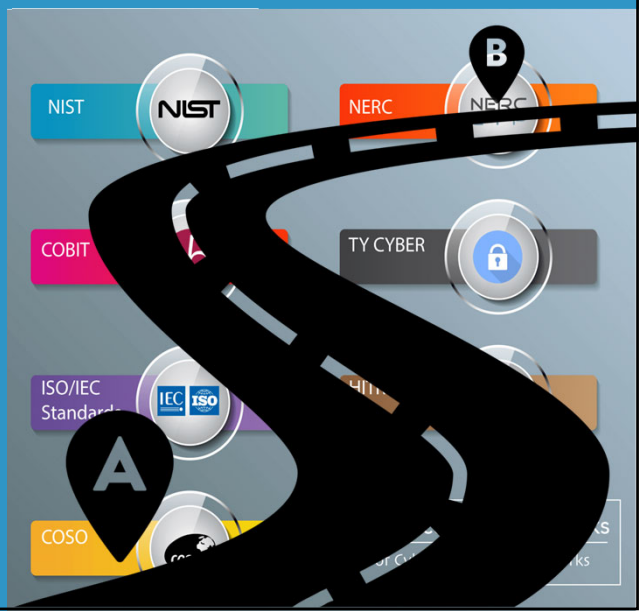
HEARTLAND BUSINESS SYSTEMS



5

THE PATH

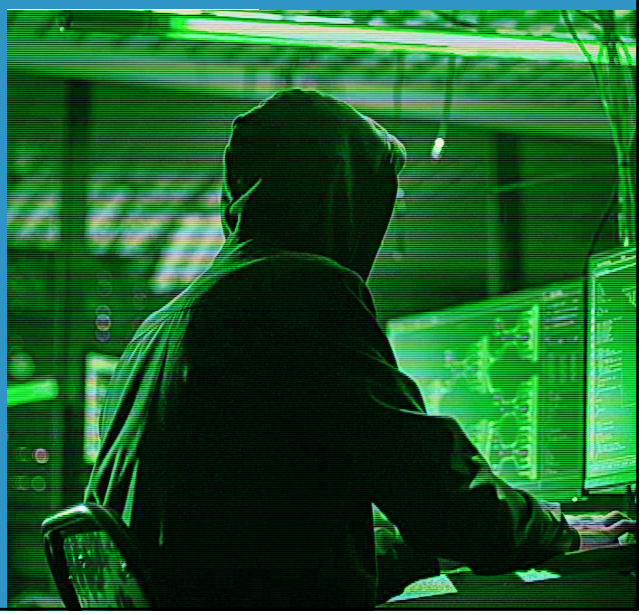
HEARTLAND BUSINESS SYSTEMS



6

THE THREATS

HEARTLAND BUSINESS SYSTEMS



7

THE HELP

HEARTLAND BUSINESS SYSTEMS

8

PRESENTERS

Todd Heinz
Director – Enterprise Security Risk Management Practice
theinz@bs.net • (262) 920-1688

Kathy Elliott O'Neil
Senior Privacy Security Consultant
kelliottoneil@hbs.net • (262) 264-6860

David Donnelli
Senior ESRM Architect & Penetration Tester
ddonnelli@hbs.net • (630) 786-6601

9

HOUSEKEEPING

- We will save time for questions
- Lot of info on slides – meant to be take home resource
- Presentation is available for download

10

ENTERPRISE SECURITY RISK MANAGEMENT

HEARTLAND BUSINESS SYSTEMS

Information Security

or

Technology Security

or

IT Security

11

ENTERPRISE SECURITY RISK MANAGEMENT

HEARTLAND BUSINESS SYSTEMS

Information Security

Risk Management

ESRM

Business Continuity

Privacy & Compliance

Security is not an IT problem … *it's an organizational problem*

12

SECURITY PROGRAM BLUEPRINT

HEARTLAND BUSINESS SYSTEMS

13

SECURITY PROGRAM BLUEPRINT

HEARTLAND BUSINESS SYSTEMS

NIST CSF

HIPAA (Health Insurance Portability and Accountability Act)

PCI (Payment Card Industry Data Security Standards)

GDPR (General Data Protection Regulation)

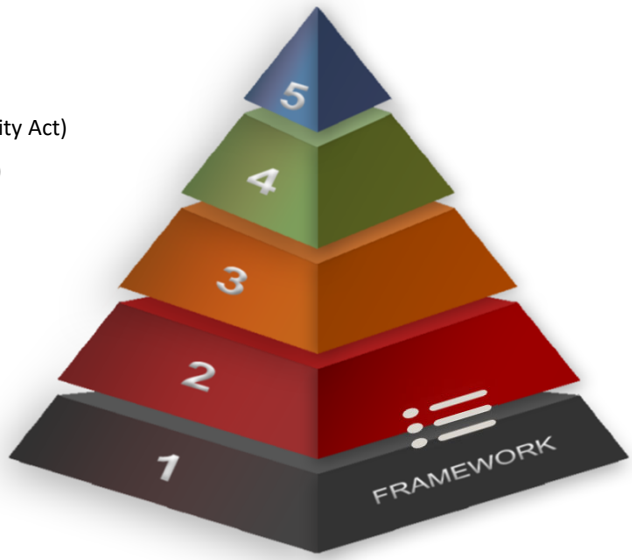
GLBA (Gramm-Leach-Bliley Act)

SOX (Sarbanes-Oxle)

NIST 800-171

NIST 800-83

etc.



14

SECURITY PROGRAM BLUEPRINT

HEARTLAND BUSINESS SYSTEMS

Sample Policies

Acceptable Use
Access Control
Anti-Malware
Asset Management
Auditing
Awareness & Training
Backup and Recovery
Business Associate/Vendor Management
Business Continuity and Disaster Recovery
BYOD
Change Management
Clear Desk
Configuration Management
Cryptography
Data Center Access
Data Classification
Data Destruction & Retention
Encryption
Exception Management
Firewall
Guest Network Access
Human Resources Security
Identity and Access Management
Incident Management
Intrusion Detection / Prevention

15

SECURITY PROGRAM BLUEPRINT

HEARTLAND BUSINESS SYSTEMS

Sample Training

End User

Executive

Administrator

Social Engineering

Incident Response

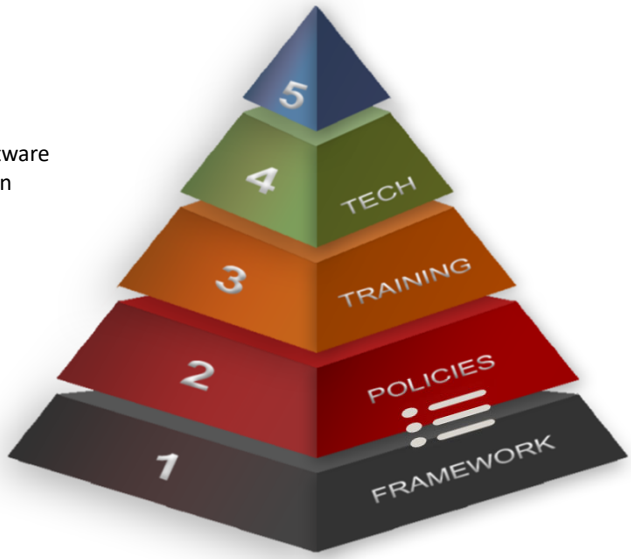
16

SECURITY PROGRAM BLUEPRINT

HEARTLAND BUSINESS SYSTEMS

Sample Technologies

Firewalls
Intrusion Prevention Software
Mutifactor Authentication
Encryption
Laptops / Servers
Routers & Switches
Anti-Virus
Smartboards
Operating Systems
Web Applications
…



17

SECURITY PROGRAM BLUEPRINT

HEARTLAND BUSINESS SYSTEMS

Governance

Risk

Compliance

18

SECURITY MATURITY MODEL

HEARTLAND BUSINESS SYSTEMS

Reactive ⟷ **Proactive**

Blocking & Tackling

- Lack of Executive support
- Underfunded
- Understaffed
- Lack of metrics for reporting
- Set up for failure

Compliance Driven

- Control-based security approach
- Align to mandatory regulations
  - EU/PII Data protection
  - FFIEC
  - HIPAA
  - ISO 2700x
  - PCI
  - NCUA

Risk-Based Approach

- Multi-layered security and risk-based approach
- Using behavior analytics and evaluating new technologies frequently
- Linking events across multiple disciplines

19

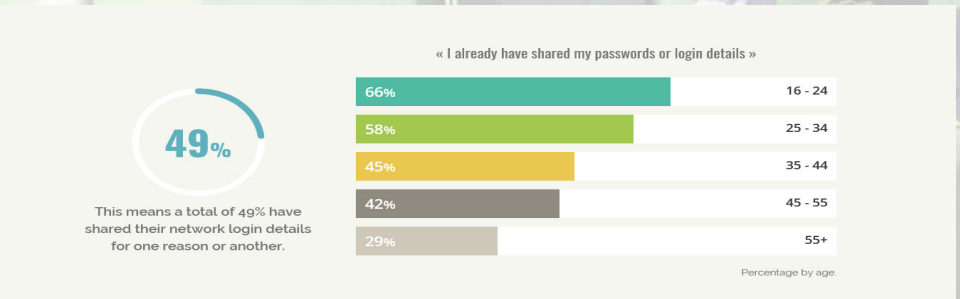
20

PASSWORDS

HEARTLAND BUSINESS SYSTEMS

Lack of strong passwords, sharing passwords, password reuse - using the same password for everything creates large gaps in your cyber security defenses.

Passwords ensure the security and confidentiality of data that is stored on workstations and severs across an organization. Some of this data includes private information about employees (e.g. payroll, reviews, etc.), confidential information about the organization (e.g. budgets, plans and programs) and students (e.g. grades, evaluations, etc.)



21

PASSWORDS

HEARTLAND BUSINESS SYSTEMS

Enforce :

- ✓ **A requirement for strong passwords -** operating system features for minimum password length can be configured to prevent user from choosing short passwords.
- ✓ **Password complexity** (requiring passwords to be a string of pseudo-random characters), built-in operating system settings or third-party password complexity enforcements tools can be applied.
- ✓ **Password management** - requiring frequency of change, time period for reuse (not number of uses)
- ✓ **Training -** to ensure everyone understands the perils of sharing passwords. And how using the same password for everything is asking for bad things to happen.
- ✓ **Training everyone** to NOT use the same password for everything (LinkedIn and Mark)
- ✓ **No one** will ever ask for your password – and never offer it
- ✓ **Source:** NIST Digital Identity Guidelines 800-63-3

22

23

OPEN ACCESS TO NETWORKS

HEARTLAND BUSINESS SYSTEMS

Laptops, computers, and other devices (mobile devices, etc.) are left unattended and open to your network.

Open access to your network and applications can create a number issues: from sabotage of your network, installation of unwanted software (like keyloggers to capture keystrokes, etc.), obtain confidential information, change your password, send out emails under your name, pretend to be you . . . .

Increase security awareness and what can happen:

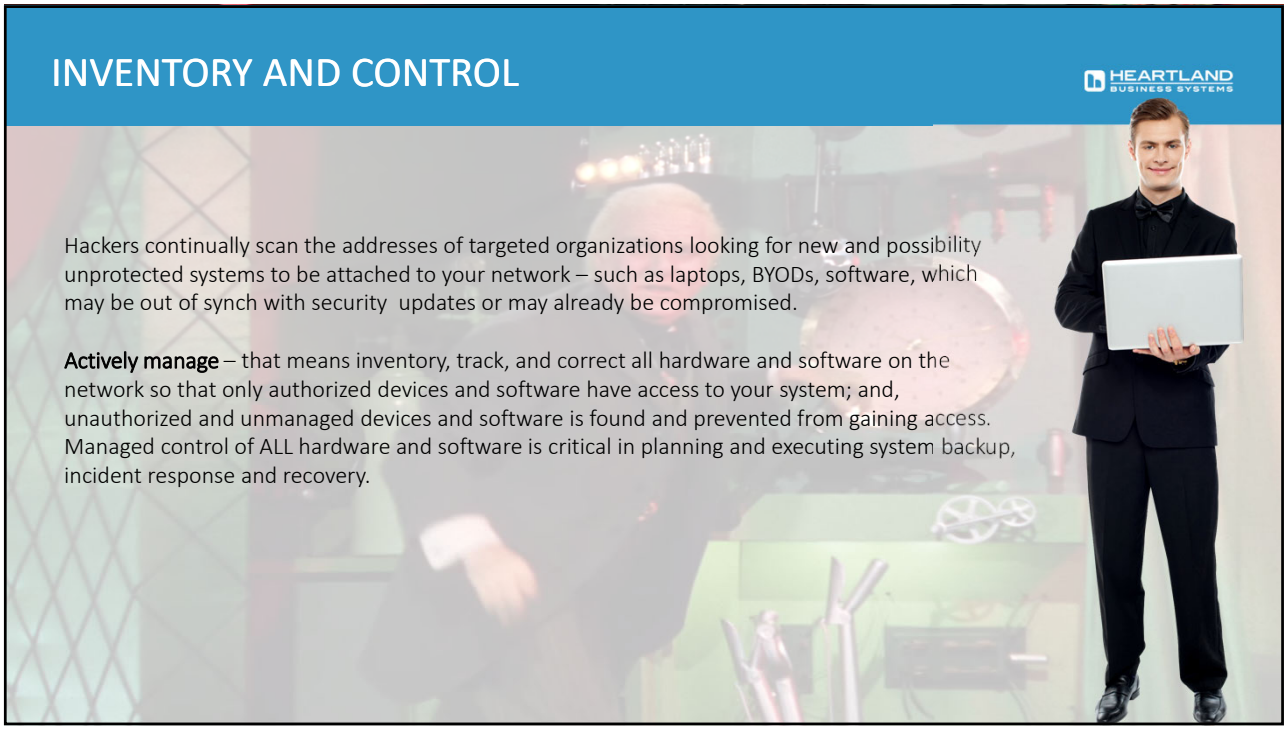
- ✓ Train everyone to lock and logout of applications and your network.
- ✓ Ensure lock-outs are implemented with minimal minutes (5 to 10 minutes).
- ✓ Laptops (and other similar devices): be sure they are encrypted.
- ✓ Walk around and check unsecured and unmonitored devices. Implement sanctions as appropriate.

24

25

INVENTORY AND CONTROL

HEARTLAND BUSINESS SYSTEMS



Hackers continually scan the addresses of targeted organizations looking for new and possibility unprotected systems to be attached to your network – such as laptops, BYODs, software, which may be out of synch with security updates or may already be compromised.

Actively manage – that means inventory, track, and correct all hardware and software on the network so that only authorized devices and software have access to your system; and, unauthorized and unmanaged devices and software is found and prevented from gaining access. Managed control of ALL hardware and software is critical in planning and executing system backup, incident response and recovery.

26

INVENTORY AND CONTROL

HEARTLAND BUSINESS SYSTEMS

- ✓ Maintain an accurate and up-to-date inventory of all technology assets with potential to store or process information (include all hardware assets, whether connected to the network or not (include each machine using an IP address, software).
- ✓ Ensure your inventory records network address, hardware address, machine name, data asset owner and department, and whether the asset/software has been approved to connect to the network, include last patch update.
- ✓ Conduct inventory scans (hardware and software) on a frequent basis.
- ✓ Ensure you know what endpoints must be protected and what software is running on those endpoints.
- ✓ Remove unauthorized assets from the network, quarantine as necessary.
- ✓ Implement whitelisting tools to ensure only authorized software versions are in use.
- ✓ Define a process and standards for new hardware and software installation: sandbox testing, isolated, documented and managed.
- ✓ Define exceptions and use a policy and standard to monitor the exceptions.

27

28

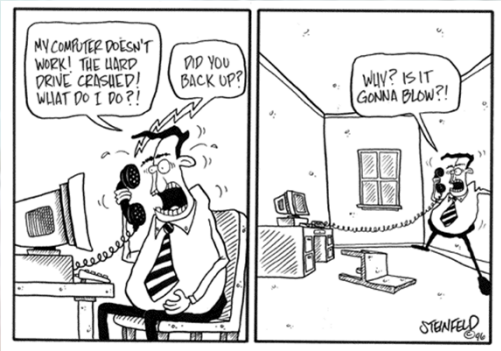
DATA RECOVERY

HEARTLAND BUSINESS SYSTEMS

Data backups are limited, not tested, and are connected to the network. When hackers compromise machines they often make changes to configurations and software. They can also make alterations to data stored on compromised machines and may pollute your information (data).

Without a process and tools to properly back up critical information you will not be able to recover on a timely basis, if at all.

- ✓ Back up your systems on a timely basis.
- ✓ Ensure that key systems are backed up as a complete system to enable the quick recovery of a entire system.
- ✓ Test the data integrity of the backup media on a regular basis by performing a data restoration process to ensure the back up is working properly.
- ✓ Protect your backups – via physical security, encryption and off your network (isolated, disconnected and offline).



29

30

SECURITY AWARENESS AND TRAINING

HEARTLAND BUSINESS SYSTEMS

It is tempting to think of cyber security as primarily a technical challenge – in reality it is about the actions of people. People play a critical part of the success or failure of cyber security – and attackers know this and target the vulnerable.

People fulfill important functions within the organizational system – from system design, implementation, operations, use and oversight. Empower people with good cyber defense habits – train them, create awareness.

31

SECURITY AWARENESS AND TRAINING

HEARTLAND BUSINESS SYSTEMS

- ✓ Perform a gap analysis to understand the behaviors and skills of your works force – build a baseline education roadmap to enhance skills and define your systems.
- ✓ Create awareness for all workforce members (all to include officials, leaders, etc.) to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization.
- ✓ Update your training annually to include new technologies, threats standards and your organizational requirements.
- ✓ Train everyone to know the importance of utilization of security authentication (passwords, role-based access to information/data, physical access to buildings, areas, server closets, etc.
- ✓ Ensure workforce members understand your sanctions for non-compliance.
- ✓ Social Media use and standards, dangers of improper use.
- ✓ Data Classification (pubic, confidential, private) and guidelines for data users/data owners.
- ✓ Login Banners – great reminders.
- ✓ Technology Acceptable Use.
- ✓ Sources: NIST SP 800-50 Infosec Awareness Training, EDUCAUSE.

32

33

POLICIES, PROCEDURES, AND STANDARDS

HEARTLAND BUSINESS SYSTEMS

Policies, procedures and standards support your security program. Without training they can not be implemented. Without implementation they are not effective.

An effective organization wide security program considers policy and technology at the same time as the training of people. Policies should be designed with technical measurement and enforcement and should be reinforced by training to fill the gaps in understanding and minimize the opportunity for mistakes. Updates and changes should be continual and follow a planned process. Consider it an ongoing process improvement to information/data, physical access to buildings, areas, server closets, etc.

34

POLICIES, PROCEDURES, AND STANDARDS

HEARTLAND BUSINESS SYSTEMS

- ✓ Training should be specific, tailored and focused on specific skills needed by the workforce to support your policies, procedures and standards.
- ✓ Training should be repeated periodically, measured and tested for effectiveness and updated regularly as policies and procedures are updated.
- ✓ Discourage, through training, the dangers of risky work arounds by including rationale for following policies and procedures (Incident Management and Disaster Planning processes and procedures).
- ✓ Ensure workforce members understand your sanctions for non-compliance.
- ✓ Define your security standards: ensure administrators understand and are trained on your standards; that standards are updated and reviewed as necessary. Typical standards should include, but is not limited to: Firewall standard, VPN standard, Peripheral System Configuration Standard, Malware Standard, Intrusion Detection Standard, Router Standard, Switch Standard, Wireless Standard, Windows Server Standard, Server Requirements Standard, Management Access and Privileges, Server Configuration Standard, Security Settings Standard, Disaster Recovery, Incident Management, Back-up Configuration, Database Standard, Workstation Standard, Network Perimeter Management and Design Standard, Event Logs Standards, Patch management Standards, Authorization Standards, etc.
- ✓ Define your set of organizational policies and procedures, write and implement them. These may be dependent upon regulatory and compliance requirements. Work with Human Resources, Legal, Security, Compliance and departments and divisions to ensure organizational alignment. Use common practices, shared policies, shared management tools across the organization increases effectiveness and responsiveness.

35

36

CYBER SECURITY ASSESSMENT & MITIGATION PLANNINFG

HEARTLAND BUSINESS SYSTEMS

- ✓ Complete a cyber security assessment to determine where your gaps are.
- ✓ Develop a mitigation plan based upon your risk analysis of your gaps and your organization's appetite for risk.
- ✓ Share with your leaders and administrations to ensure there is management understanding of gaps, risks, and the plan to move forward.
- ✓ Define your Personnel security standards: only authorized personnel documented and allowed access to your data assets (consider workforce, consultants, and vendors).
- ✓ Ensure background checks are performed against all personnel prior to granting access and on a routine basis going forward. Think about vendors and consultants.
- ✓ Termination practices are well defined, documented and strickly and quickly performed.
- ✓ Access to data is regularly reviewed to ensure that only authorized individuals have access.
- ✓ Clarify and document your Risk Management Program and Plan (using information and data from your assessments, vulnerability and penetration testing, etc.).

37

CYBER SECURITY ASSESSMENT & MITIGATION PLANNING

HEARTLAND BUSINESS SYSTEMS

- ✓ Complete a cyber security assessment to determine where your gaps are.
- ✓ Develop a mitigation plan based upon your risk analysis of your gaps and your organization's appetite for risk.
- ✓ Share with your leaders and administrations to ensure there is management understanding of gaps, risks, and the plan to move forward.
- ✓ Define your Personnel security standards: only authorized personnel documented and allowed access to your data assets (consider workforce, consultants, and vendors).
- ✓ Ensure background checks are performed against all personnel prior to granting access and on a routine basis going forward. Think about vendors and consultants.
- ✓ Termination practices are well defined, documented and strickly and quickly performed.
- ✓ Access to data is regularly reviewed to ensure that only authorized individuals have access.
- ✓ Clarify and document your Risk Management Program and Plan (using information and data from your assessments, vulnerability and penetration testing, etc.).

38

MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS

HEARTLAND BUSINESS SYSTEMS

- ✓ Ensure your Incident Response, Management and Practice Policies and procedures are detailed, documented and exercised. Include roles, contact with law enforcement, communication strategy, documentation strategy, business contacts, vendor contacts, along with items are covered.
- ✓ Define your audit program considering your exposure and any compliance or regulatory requirements.
- ✓ Ensure you log all authentication events for both successful and unsuccessful attempts to authenticate.
- ✓ Actively monitor, log and investigate "conditions of weirdness" (COWs).
- ✓ Complete Vulnerability Scans (internal and external) on a regular basis and document results and items to be acted upon (remediated).
- ✓ Complete Penetration Testing and high-risk concerns remediated and documented. Integrate the results into your Risk Management Program and Plan.

39

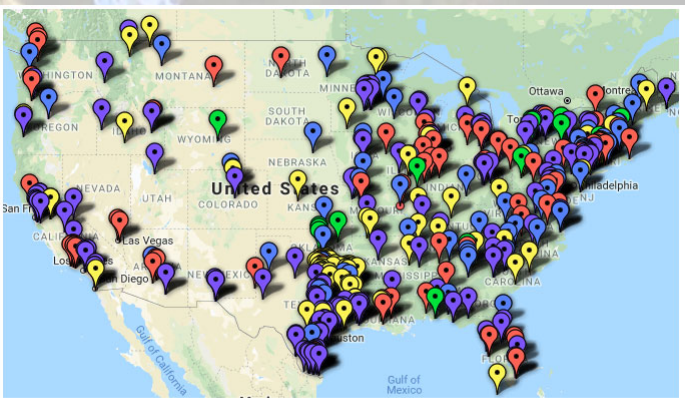
40

K-12 CYBER INCIDENT INFORMATION

HEARTLAND BUSINESS SYSTEMS

The K-12 Cyber Incident Map and underlying database captures detailed information about two inter-related issues:

1. publicly disclosed cybersecurity incidents affecting public K-12 schools, districts, charter schools, and other public education agencies (such as regional and state agencies), especially those that occur on K-12 managed networks and devices.
2. The characteristics of public school districts (including charter schools) that have experienced one or more publicly disclosed cybersecurity incidents.



The K-12 Cyber Incident Map has identified 418 incidents since 2016 involving public schools across the United States (as of January 29, 2019).

- **MAP KEY**
- phishing attacks resulting in the disclosure of personal data (blue pins);
- other unauthorized disclosures, breaches or hacks resulting in the disclosure of personal data (purple pins);
- ransomware attacks (yellow pins);
- denial-of-service attacks (green pins); and
- other cyber incidents resulting in school disruptions and unauthorized disclosures (red pins).

https://k12cybersecure.com/year-in-review/2018-data/

41

42

DATA BREACHES

HEARTLAND BUSINESS SYSTEMS

- According to CDW's recent Cybersecurity Insight Report 46% of all organizations have experienced a serious data breach.
- The most frequently experienced type of K-12 cyber incident reported in 2018 were data breaches.
- What constitutes a data breach?
  - Unauthorized disclosures of data by current and former K-12 staff, primarily—but not exclusively—due to human error.
  - Unauthorized disclosures of K-12 data held by vendors/partners with a relationship to a school district.
  - Unauthorized access to data by K-12 students, often out of curiosity or a desire to modify school records (including grades, attendance records, or financial account balances).
  - Unauthorized access to data by unknown external actors, often for malicious purposes.

43

DATA BREACHES

HEARTLAND BUSINESS SYSTEMS

Why the Education sector?

- School districts are considered "soft targets" by cybercriminals for multiple reasons.
- School districts must do what is necessary to restore day-to-day services as quickly as possible after attacks. These organizations are thought to be more likely to pay ransoms or give cybercriminals what they want.
- Your information is valuable. A child's identity is extremely attractive to identity thieves because it is a clean slate. Thieves use a child's Social Security number to obtain employment, government benefits, or credit without detection until the child is of age to obtain credit.
- Cybercriminals realize that many school districts face budget shortfalls and have a wide range of other expenses that take priority over cybersecurity.

44

DATA BREACHES

HEARTLAND BUSINESS SYSTEMS

Tips

Tips to prevent data breaches

Implement SSL Decryption/Inspection

- SSL/TLS encryption and decryption is becoming an important part of network security. In 2017, 50 per cent of web traffic was secured by the protocol, and Gartner expects this to rise to 80 per cent by 2019.
  - Educational institutions must protect their students and infrastructure from malware, ransomware, and other threats hiding in SSL/TLS encrypted traffic. Cyber attackers may also use encrypted traffic to disguise attempts to extract sensitive data. Educational institutions may be required by law to keep students and the school from illegal behavior or material hiding in SSL encrypted traffic.

Implement Multi-Factor Authentication

- Multi-Factor Authentication works to thwart cybercriminals by requiring additional information or credentials from the user. A phishing attack may garner a user's credentials, but it won't provide the hacker with a fingerprint, for instance, or the answer to a personal security question.
- Similarly, a brute force or reverse brute force attack may manage to find a working username and password, but the attacker doesn't know what other authentication factors the MFA system requires and doesn't have those credentials.

45

DATA BREACHES

HEARTLAND BUSINESS SYSTEMS

Have you been PWNED?
https://haveibeenpwned.com/

Website where you can check if you have been part of one of the major data breaches.

346	6,931,949,148	90,436	111,599,387
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
161,749,950	Dubsmash accounts
152,445,165	Adobe accounts

Recently added breaches

40,960,499	ShareThis accounts
161,749,950	Dubsmash accounts
143,606,147	MyFitnessPal accounts
91,991,358	MyHeritage accounts
19,611,022	EyeEm accounts
1,508	devkitPro accounts
772,904,991	Collection #1 accounts
87,633	FaceUP accounts
4,848,734	Dangdang accounts
213,415	BannerBit accounts

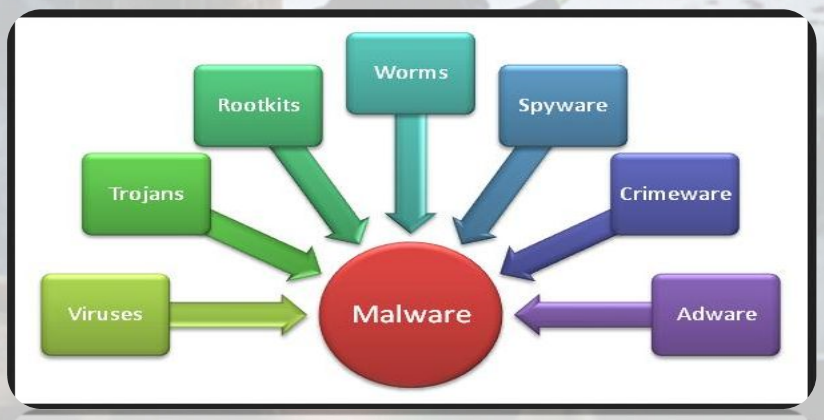
46

47

MALWARE

HEARTLAND BUSINESS SYSTEMS

What is the difference between Malware and Viruses/Spyware/Adware/etc.?



48

MALWARE

HEARTLAND BUSINESS SYSTEMS

Malicious Cryptomining (CryptoJacking)

- The theft of computer processing resources — electricity, cloud services and other digital assets — that are then exploited to do cryptocurrency mining without the owner's permission or knowledge

Ransomware was dethroned in the first half of 2018 to make way for a massive wave of cryptominers, following a meteoric spike in Bitcoin value at the tail end of 2017.

- Threat actors seemingly abandoned all other forms of attack for experimentation in this new technique, spanning from desktop to mobile.
- While the largest targets are made up of energy and utility companies, in a recent Cisco study, colleges experienced 22 percent of all cryptomining attempts, while K-12 made up 4 percent of the total.

49

MALWARE

HEARTLAND BUSINESS SYSTEMS

Malicious Cryptomining Facts

- Malicious cryptomining malware activity rose by over 4000 percent in 2018, according to a new quarterly report published by McAfee Labs, Dec. 18.
- New [mining] malware targeting IoT devices grew 72%, with total malware growing 203% in the last four quarters. New coinmining malware grew nearly 55%, with total malware growing 4,467% in the last four quarters
- According to the Malwarebytes team, Malwarebytes products have blocked on average around 8 million requests per day to domains hosting in-browser cryptocurrency mining scripts.
- Cyber-security firm Ixia published a case study of a few Android apps that also pushed cryptocurrency miners onto the uses devices.
  - These Apps were listed on the Google Play Store.
  - https://www.ixiacom.com/company/blog/everythings-better-blockchain

Malwarebytes Labs 2019 State of Malware Report

Top North America Detections 2017/2018

Business		Pos.	Consumer	
Y/Y	Threat		Threat	Y/Y
99%	Trojan	1	Adware	-19%
33%	Hijacker	2	Trojan	7%
121%	RiskwareTool	3	RiskwareTool	38%
29%	Adware	4	Backdoor	10%
82%	Spyware	5	Hijacker	-41%
11%	Backdoor	6	Spyware	18%
-27%	Worm	7	HackTool	-40%
-15%	Ransom	8	Rogue	-35%
-55%	Rogue	9	Rootkit	-50%
-64%	Rootkit	10	Virus	-57%

50

MALWARE

HEARTLAND BUSINESS SYSTEMS

If people are making money through Malicious Cryptomining is Ransomware on the way out?

- No Ransomware is still the top variety of malicious software found in 39% of cases where malware was identified. (Verizon 2018 DBIR)
- New viruses & trojans will review a systems configuration and based on what it finds deploy either a ransomware or cryptominer attack.
  - Many of these will examine a system for crypto currency wallets. If a wallet is not found it will move from ransomware to malicious cryptomining.
  - This is a way to maximize profits from victims, since not all ransomware victims pay the ransom after encryption. The presence of a crypto currency wallet could signify that the user is capable of paying the ransom and that the system holds valuable information that can be held hostage.

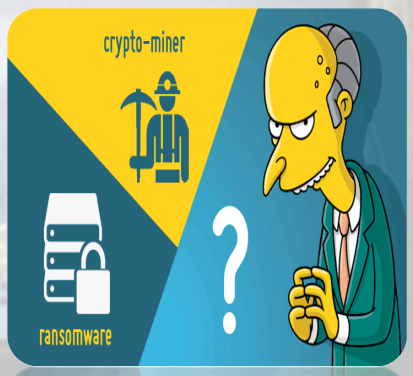
51

MALWARE

HEARTLAND BUSINESS SYSTEMS

How can I protect myself?

- ✓ Employ a good web filtering/protection system.
  - ✓ SSL Decryption.
- ✓ Keep an offline or unmounted backup of your system.
- ✓ Employ client and server malware protection software.
- ✓ Employ a security awareness training program.
- ✓ Setup a centralized logging and alerting system.
- ✓ Retire legacy equipment.



52

MALWARE

HEARTLAND BUSINESS SYSTEMS

Notes from the field – EternalBlue

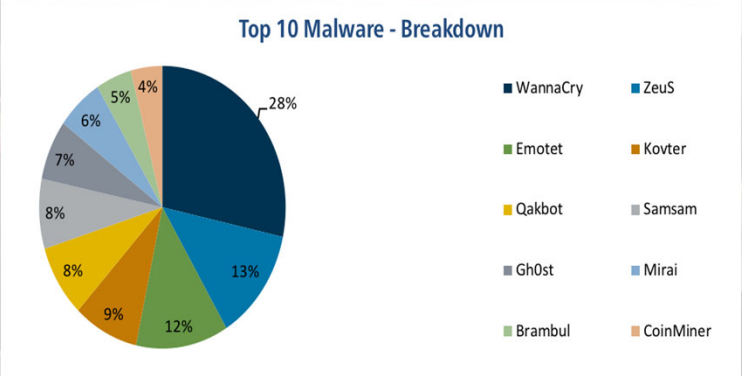
- EternalBlue – The exploit that has been patched yet won't die.
  - Petya/NotPetya/WannaCry/CoinMiner
- The EternalBlue exploit was released to the public in 2017 as part of a leaked cache of surveillance tools owned by the NSA's hacking team.
- Hackers called the "Shadow Brokers," compromised NSA systems and leaked the toolset.
- According to multiple reports at the end of 2018, millions of systems were still vulnerable to EternalBlue.
  - This has led to millions of dollars in damages due primarily to ransomware worms. Following the massive impact of **WannaCry**, both **NotPetya** and **BadRabbit** caused over a billion dollars worth of damages in over 65 countries, using EternalBlue as either an initial compromise vector or as a method of lateral movement.

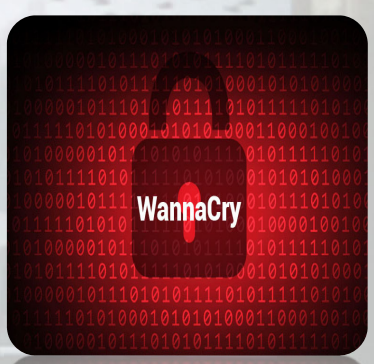
53

MALWARE

HEARTLAND BUSINESS SYSTEMS

CIS Center for Internet Security Top 10 Malware Infections December 2018





54

MALWARE

HEARTLAND BUSINESS SYSTEMS

Why won't EternalBlue based attacks Die?

- Unpatched PCs are a key reason EternalBlue won't die, with impacted devices "getting stuck in an endless infection cycle with new infections occurring at the kernel level as the previous ones are removed."
- Legacy protocols not being disabled. **(SMBv1 specifically)**
  - Link on how to disable SMBv1:
    - https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and
- Other legacy protocols that should be disabled:
  - SSLv2 & v3
  - TLS 1.0 & 1.1
  - LanMan (LM) / NTMLv1
  - Digest Authentication.

55

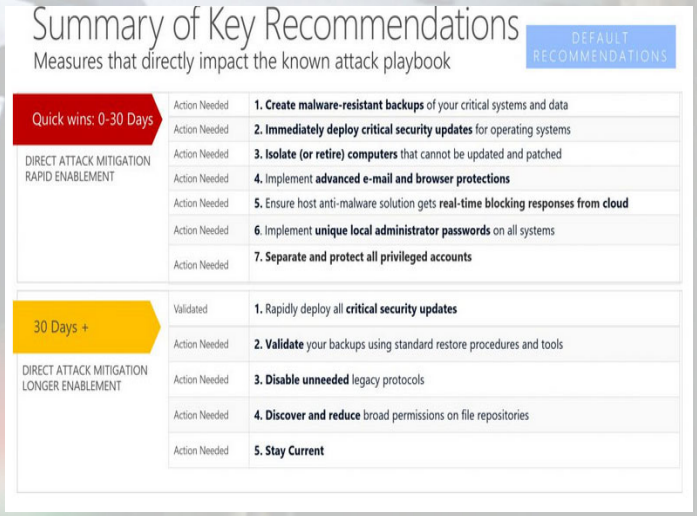
MALWARE

HEARTLAND BUSINESS SYSTEMS

Microsoft lends a helping hand!

Microsoft Rapid Cyberattack Assessment.

- Designed to help organizations understand the potential vulnerabilities and exposures they have to ransomware attacks so that they can take steps to keep from being the next victim.
- This assessment takes you through 12 multiple selection questions, runs a scan of your environment and produces a report w/supplemental documents that detail risks to your environment
  - In that report you also get recommendations in a 0-30 Days and 30+ Day format.



Summary of Key Recommendations

Measures that directly impact the known attack playbook

DEFAULT RECOMMENDATIONS

Quick wins: 0-30 Days DIRECT ATTACK MITIGATION RAPID ENABLEMENT	Action Needed	**1. Create malware-resistant backups** of your critical systems and data
	Action Needed	**2. Immediately deploy critical security updates** for operating systems
	Action Needed	**3. Isolate (or retire) computers** that cannot be updated and patched
	Action Needed	**4.** Implement **advanced e-mail and browser protections**
	Action Needed	**5.** Ensure host anti-malware solution gets **real-time blocking responses from cloud**
	Action Needed	**6.** Implement **unique local administrator passwords** on all systems
	Action Needed	**7. Separate and protect all privileged accounts**
30 Days + DIRECT ATTACK MITIGATION LONGER ENABLEMENT	Validated	**1.** Rapidly deploy all **critical security updates**
	Action Needed	**2. Validate** your backups using standard restore procedures and tools
	Action Needed	**3. Disable unneeded** legacy protocols
	Action Needed	**4. Discover and reduce** broad permissions on file repositories
	Action Needed	**5. Stay Current**

56

57

PHISHING

HEARTLAND BUSINESS SYSTEMS

Phishing Facts

- In a survey of over 1,300 IT decision makers, 56% of organizations identified targeted phishing attacks as their biggest current cybersecurity threat. (CyberArk)
- 76% of businesses reported being a victim of a phishing attack in the last year. (Wombat Security)
- Verizon reports that users in the U.S open 30 percent of all phishing emails.
  - 12 percent of those targeted by these emails clicking on the infected links or attachments. (Verizon)
- Kaspersky's Anti-Phishing system was triggered 246,231,645 times in 2017. The security company states over 91 million more phishing system triggers were set off in 2017 over 2016. (Kaspersky)

58

PHISHING

HEARTLAND BUSINESS SYSTEMS

To the Phishing Rescue

- Typical K-12 phishing baseline click rate is 20-60%
- Education industry benchmark is 2%
- 3 months after security awareness training, click rate is 13-18%
- 12 month after security awareness training, click rate is around 2%

More than 90% of cyber breaches are due to successful phishing attempts

KnowBe4

99 Recipients	100% 99 Delivered	62.6% 62 Opened	56.6% 56 Clicked	0% 0 Replied	0% 0 Attachment Open	0% 0 Macro Enabled	0% 0 Data Entered	0% 0 Reported	0% 0 Bounced

59

PHISHING

HEARTLAND BUSINESS SYSTEMS

Acknowledgements / Resources

- https://studentprivacy.ed.gov/
- https://k12cybersecure.com/
- https://thehackernews.com/2018/07/cryptocurrency-mining-ransomware.html
- https://gdpr.report/news/2019/01/23/report-reveals-the-dangers-and-trends-of-malware-through-2018/
- https://cointelegraph.com/news/crypto-mining-malware-up-over-4-000-in-2018-says-mcafee-report
- https://www.versa-networks.com/new-report-reveals-top-10-cryptomining-malware-2018/

60


QUESTIONS?

61


THANK YOU !
Please download this presentation
on https://brainstormk20.com/wisconsindells/

62